1076

DECLASSIFIED
Authority NW 48901

INTERROGATION OF OBLT. SCHUBERT (OKH/CHEF HNW/GEN. d. NA.) ON RUSSIAN MILITARY AND AGENTS' SYSTEMS

This report comprises:

(a) Interrogation of Oblt. Schubert on 17/6/45 at OKM Signal School. Flensburg, by Captain Royffe, I.C.

(b) Supplementary notes by Captain Royffe.

(c) Complete translation of a paper written by Oblt. Schubert at Flensburg, and dated 19/6/45, on Russian Agents' Systems, and on those of the Polish National Resistance Movement.

A report of the initial interrogation of Schubert has already been issued as TICOM/I-15.

TICOM
4 July 1945.

Copy No. 16
No. of Pages 15

Distribution:

British
1. Director
2. D.D.3.
3. D.D.4.
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8. A.D.(C.C.R.) (2)
9. Lt.Col. Leathem

TICOM
10. Chairman
11-12. S.A.C. (2)
13. Cdr. Bacon
14. Cdr. Mackenzie
15. Cdr. Tandy
16. Lt.Col. Johnson
17. Lt.Cdr. Manson
18. Major Seaman
19. Lieut. Eachus
20. Lieut. Vance
21. Captain Cowan
22. Lieut. Fehl
23-25. TICOM Files (3)

U.S.
26-27. OP-20-G (2) (via Lt. Pendergrass)
28. G-2 (via Lt.Col. Hilles)
29-30. S.S.A. (2) (via Major Seaman)
31-32. Director, S.I.D. ETOUSA (2) (via Lt.Col. Johnson)

Additional
33-35. Lt.Col. Pritchard (3)
36. Major Morgan.
37. Captain Royffe

Do NOT Destroy this Publication
NSA Technical Library when no longer needed
Copy No. 2
S-4527

NSA Technical Library when no longer needed
S-4527
Copy No. 2

Declassified by NSA/CSS
Deputy Associate Director for Policy and Records
On 20130401 by

DECLASSIFIED
Authority NW 48901

T26

TOP SECRET "U"

INTERROGATION ON 17/6/45 P.M.

Q.1 Can you give us first a resumé of your work in the organisation?

Oblt. Schubert: Perhaps the best way is for me to give you the more important personal details, and you can gather from that the extent of my information. I entered the Sigint Service when I was called up for my military service in 1937, and was first an intercept and D/F operator, until the close of the French campaign, in a Signals Intelligence Company which was then commanded by Hptm. SEEBOHM and later went to Africa. Then at the beginning of 1941 I went to the Signals School and became an officer, and was next with the Signals Recce Replacement Abteilung, at that time in Frankfurt/M. In the winter I was given leave in order to study; for the rest of the time I was instructor and adjutant. After my studies I was posted to a cryptanalytic course at OKH. Since then I have functioned as a cryptanalyst. I joined Sigs Recce 6 (Note 1) and took part in the Caucasus campaign. I worked on Russian Army till March 1943. Then Kommandeur 6 was given the commitment of covering the Russian partisans, and I worked on that till September of that year. After that Kommandeur 6 was dissolved and I went with the crypto party to OKH to "General der Nachrichtenaufklaerung" and there took over all Eastern Cryptanalysis (Note 2) which dealt with NKWD and partisans. In addition to this, I was ordered at the beginning of this year to take over a review on the various British and American cyphers. I was then posted from the end of February until the middle of April to the Navy to make myself familiar with Naval cyphers.

When I wanted to return to OKH, the separation between North and South had taken place; I was taken to the North and therefore remained there. Originally then, the intention was that I should return to OKH, while the zones had not yet been decided on.

Q.2 Can you describe the Russian Army system to us?

Oblt. Schubert: The Army cyphers have been continually strengthened since the Russian campaign began. Cyphers at the beginning of the campaign against Russia were rather primitive. For practice keys, i.e. for messages which have no operational content, a simple system was adopted of substituting 2 figures for each letter. These systems were known originally for the whole Army uniformly as PT 39. They were then replaced by PT 41 and PT 41 N. There were squares 10 x 10 containing letters and figures. Recypher strips changed daily (Note 3).

Last year there were various codes in use. Keys were compiled by the different Cypher Departments in whose territory they were used. As regards other forward keys it can be said that their basic construction is the same as that for the Air Force and the Navy. Compilation of individual keys was again at times the commitment of the Cypher Dept., where they were to be used. Directives on this point were issued by the Central Cypher Dept. of the Red Army and the Cypher Departments of the units had to conform to these directives.

Declassified by NSA/CSS
Deputy Associate Director for Policy and Records
On 20130401 by 85

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

Q.3 Were you in touch with the Naval organisation?

Oblt. Schubert: I endeavoured to achieve cooperation between the Army and the Navy. This task was actually no concern of mine. A naval officer was detached for 6 weeks who looked at all Army systems originating in the West and the East and I went to him to attempt some settlement. I tried to achieve collaboration but later events upset things. There are practically no points of contact between Army and Navy - as regards the Russians. There was good cooperation with the Air Force in that the "Kommandeure der Nachrichtenaufklaerung" situated with Army Groups worked with the corresponding Air Sigint Abteilungen and furthermore cryptographers at the HQ of the Sigint Unit (Leitstelle der N.A.) worked with the Regiment operating by orders of the Luftwaffe on Eastern Sigint in the East. This was Air Sigint Regt.353.

Q.4 Will you now describe the 4-figure cypher?

Oblt. Schubert: The Russian Army keys are 3 or 4-figure systems. The basis is the same. They are small codes of 300-800 positions - more in some cases. In general small scope but frequent change. Recyphering is done by substitution tables - e.g. if the 4 figures of the code are described as a, b, c, d, then in the 4-figure code 2 figures went together i.e. a-b, b-c, or c-d, representing the page of the code-book. This pair was substituted by a bigram substitution table. There are perhaps in the code only 6 or 7 actual pages, but each page has a block of consecutive numbers, e.g.:-

Page 01 becomes 11 - 23 (Note 4)

Page 02 becomes 00 - 10 etc.

Recyphering of the other two figures was also done by single-figure substitution tables, so that either one figure was always substituted by one other or that in the actual code only 5 different figures could appear, each having two alternatives, e.g. 5 = 4 or 8.

It often happened that the different recyphering tables used were found to run systematically one after the other. For example, that Section 11 - 23 always went together. In most cases the indicators could be recognised at the beginning of a message and there was no further recyphering of the indicators. For example in the 4-figure cypher the indicator was 1408 and occupied the 3rd place. Two figures indicated which substitution table had to be used for the page, and two the tables for the position. It might also happen that one of the 4 figures had no significance and one figure alone indicated which column had to be chosen for the position, or the figures 14 - 25 might all indicate the same substitution table. There were sometimes 2 indicator groups, each bigram indicating a substitution table.

Recently the Russians went over more and more to using new indicator groups for each message so that it became increasingly difficult to find messages on the same key.

The 3-figure cypher is quite similar to the 4-figure apart from the fact that the substitution tables are all single-figure. It was customary to mix clear and cypher text, i.e. times etc. would be given en clair. Co-ordinates were always given in a special key, not contained in the code. These co-ordinates were noticeable in that whereas the code was 3-figure the co-ordinates were 5 or 6-figure.

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

126

Towards the end, in addition, there appeared quite isolated 4 to 7-figure substitution systems - presumably private systems of the respective Cypher Depts. I imagine this to be so as they appeared very seldom.

Q.5 Can you describe the NKWD systems?

Oblt. Schubert: Various cyphers were used in NKWD traffic. We covered the Security Troops' traffic. These are the NKWD bodies which are situated in rearward areas of Armies, in order to defend base Army areas. Then NKWD Frontier Troop cyphers, who were operating on the neutral frontiers of Russia. Then NKWD Railway and Convoy Troops responsible for defence of lines of communication. In addition one or two cyphers of NKGB are known to me. This is the 4th Section of the NKWD. This Section concerned itself with measures against enemy agents and own active espionage. Operation of own agents was handled in the main through NKWD Organisation SMERSCH. I don't know if there are any more. I have merely mentioned those with which I came into contact. There are two different cyphers in use with the NKWD Security Troops. The first one works forward of Regiment, when a regiment is used in approx. an Army Group sector. It is a cypher, therefore, used forward of Army Group. There is a further cypher used back from Regiments to Central Office or Station, via Divisional Staffs. Cypher forward of Regiments was a 4-figure code, running for a comparatively long period. The last one which was still valid in the middle of February when I left OKH, had already been running 1½ years. This code was alphabetical and was recyphered as follows. There are 100 pages and on each page - I don't remember the details now - there were 25 or 50 positions. I think 25. The recypher was shown by an indicator group, which was also re-cyphered. Two figures of this gave the substitution table to be used for the page, the third figure indicated an additive for the "position" on the page. For example, Indicator figure 5. On page 01, 3 is to be added to every position figure so that position 01 - 01 became 01 - 04. On page 02, 4 is to be added so that 02 - 02 became 02 - 06. And so on, different for every page. This adder is always one digit i.e. only 0 - 9 and fixed for every page by these indicator group figures. There are therefore 10 different possibilities of this sort; the figures recyphered by the adder are then changed again according to another substitution table, indicated by the 4th figure of the indicator group. The substitution tables used were valid for a longish time and varied with the network. For instance different sub-stitution tables were used on the White Russian Front from those on the Baltic Front. The adders on these pages were not variable. Only the substitution table changed. Indi-cators were so arranged that a certain figure in one group showed where a specific group was to be taken out of the message. For example the third group from the end indicated by its last figure which group of the message was to be used for recyphering. The group so shown was then added to the clear indicator and the result inserted in a certain place.

Rearwards of Regiments there was another 4-figure code, re-cyphered with a figure subtractor. This subtractor was originally taken from tables (up to Sept. 1944) which were different on different networks but the same tables might appear later in other networks. As the table only contained a limited stock of groups, it happened that the subtractor was used very frequently and it was not uncommon for 20 messages to have the same subtractor. It may be accepted

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

126

that up to the middle of last year the Russians did not realise that code messages using the same subtractor are breakable if the code is not known. In contrast to the Army, which changed its codes frequently and exercised great care with the subtractor, the NKWD thought themselves safe with their cyphers as valid NKWD codes were never captured. This cypher was changed on the 1st October last year. Instead of the single subtractor, 2 appeared, taken from different tables, and the indicators for the 2nd subtractor were recyphered with the first one. This change was a complete failure in that encoders often left the two subtractors in fixed relations to one another and it still happened that over 20 messages had the same two subtractors. We did not fully reconstitute the table up to 15th February this year. I don't know what progress there was after that date. The difficulty of recognising that two messages had the same subtractor was very easily overcome: the first group of every message was always the address, so that it was only necessary to sort messages on the first group. Recyphering of the indicator groups had not been completely clarified when I left. It was certain that those for the second subtractor were recyphered with the first. Recyphering of the indicator groups for the first subtractor had not been broken.

A 5-figure cypher, known to me, is the SMERSCH Organisation cypher (= Operation of Russian agents - SMERSCH = to smash). I myself have not worked on this cypher. Those who have, told me it is an individual subtractor. Another 5-figure cypher of the NKWD is the Railway Troops Cypher. This is actually a 4-figure code, which is recyphered by substitution tables in exactly the same way as the 4-figure code used forward of Regiments, except that the page adder is not used and each page is divided into 4 quadrants. The 5th figure indicates the quadrant in which the group appears.

The Frontier Troop cypher is exactly similar to the Security Troops cypher rearwards of Regiment, with the difference that there is a different basic book. I am only acquainted with traffic from Leningrad. To discuss this traffic is not really a NKWD subject but rather one in close association with partisan traffic. Activity of NKGB corresponds completely with the activity of spy groups which were dropped by Front HQ of the Red Army into the hinterland. These NKGB men were paratroops who were dropped in the rear of the German Army with the prime task of penetrating into counter espionage camps and of putting their services at the disposal of the German counter espionage organisations so that they could lay their hands on all persons employed by "Counter Espionage". The codes belong to the partisan and spy group categories. These are small sections, dropped from the air by parachute and on the orders of forward H.Q.s carried out recces and sabotage tasks.

Q.6 Can you say anything about agents' codes? (Note 5)

Oblt. Schubert: The cyphers were:-

1. Double transposition.

2. Subtractor.

Double transposition was only used by partisans and not by spies. The subtractor system most in use until the end was one having the subtractor printed on a teleprinter roll.

DECLASSIFIED
Authority NW 48901

TOP SECRET "U" 126

The number of the roll used was given in the message and also the group of the roll which preceded the first subtractor group, i.e. the group so given was not used as a subtractor. After encyphering, the used strop had to be torn off and destroyed. The system was completely unbreakable. Different rolls were used for the various directions of the W/T traffic.

Then there were systems in which the subtractor was taken from a table, or the subtractor could be derived from the indicator groups of the message by calculations. One could talk a whole day describing these methods. There was in existence a report of over 50 typed pages, also made accessible to the Finns. Many of the rolls turned up in captured material and were passed on to me by Abwehr units. I thought at first they were texts, converted by a simple substitution into figures. This assumption was not confirmed. On individual rolls it could be seen that the same figure must have been typed either in different sorts of print or by machines using different sorts of type faces. All figures appeared, but varied in frequency. For example, 1 would appear 15% and 7 - 5%. However, it was noticeable that this frequency fluctuated within the same roll, so that it only held good for sections of the roll - not for the whole roll. Furthermore, there were no fairly long repeats in the figure groups which could have indicated parallels in a text. This is the characteristic demonstrating that there was no clear text.

Q.7 What sort of clear text?

Oblt. Schubert: It was originally thought that these rolls were derived from a book text by substituting one figure for one letter. This was not borne out. I stopped research on the principles of these rolls because probably even if one knew the principle it would have been impossible to break the message. It was absolutely clear that the rolls must have been prepared on different machines.

There were various methods for subtracting, using subtractor tables. The simplest was a table of 10 x 30 groups, 10 columns, 30 rows and an indicator showed where one had to start reading the subtractor, e.g. indicator 24 would mean that the first 24 groups had to be struck out, and the remainder used cyclically. There was rarely enough depth to break these tables. Recyphering the indicators is a special subject which I should like to finish with. There were 6 or 7 systems, spread over all types of traffic. The basic substitution process for clear-text was always one which converted the letters into 1 or 2 figures.

The second method of taking the subtractor from a table was the one where a double subtractor was used; in fact the first subtraction came from the first 18 rows of the table and the second subtraction from the remaining 12 rows. The second subtraction always began with the first group of the 19th row. The starting point of the first subtractor was given in the indicator group. This cypher was broken. A further variation of this table appeared in the traffic from NKWD, Leningrad. It was 100 different subtractor tables of 100 groups. The first two figures of the indicator showed which of these tables was to be used. The indicator always consisted of 5 different figures and also changed the basic substitution; the indicator was written over a key-word and one filled in the remaining figures.

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

Q.8 Do you know of any cyphers used by the Polish resistance movement?

Oblt. Schubert: That was partly solved, for example some traffic was read at the time of the Warsaw Rising, and showed that it was directed not by the Russian Poles but by the London Poles. (Note 5).

W.J.O.

Note 1: He was Kommandeur der Nachrichtenaufklaerung 6. Each regiment was designated by a number, and its particular Nachrichtenaufklaerungskompanie took that number.

Note 2: There were actually three branches of the Ostentzifferung OKH: (1) Heer; (2) NKWD; (3) Partisan.

Note 3: These Leisten were strips containing co-ordinates for the sides of the square, e.g.

2 6 9 4 3 1 8 7 5 0 2 6 9 4 3 1 8 7 5 0

These could be slid according to an order indicated by the Indicator.

Note 4: The code book was cut away at the top and side margins, position co-ordinates for the pages being printed on the cover. At the bottom, the pages were thumb-indexed, page 00 having, for example, 11 - 23, and so on:

11-23	00-10	36-46	82-94

Note 5: This subject is dealt with more fully in Oblt. Schubert's paper on Agents' Systems.

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

126

SUPPLEMENTARY NOTES

Oblt. Schubert was asked to describe the different links on which the various Agents' systems were used. He said he could not remember enough to give details, which were in many cases not known. In the middle of last year, for example, the Russians had, he thought, about 3,000 agents spread over all areas, and it was impossible to pick out one system and say that was used in one area. Moreover, he himself had only worked on Partisan traffic and Kundschafter, and knew of other systems (e.g. Balkan) only indirectly.

Machines: Oblt. Schubert said he himself had never worked on machines, which were dealt with by the machine section. The Russians had a machine in use already at the beginning of the war, but not on military traffic. Recently there had been small quantities of 5-letter military traffic, but not enough to work on, and they had no idea of the system.

The T/P traffic had been worked on in the machine section, and he thought messages in depth had been read; he did not know whether the machine had been recovered.

* * * * * * *

Regarding Agents' Traffic, he mentioned that in January this year a Reg.Rat (? Ober Reg.Rat) WENZEL was sent to him from the Forschungsamt by WNV Fu 3, which was in charge of Agents' systems, with the object of collaborating with him on Polish Resistance Movement traffic. Schubert knew the Forschungsamt had worked on Polish systems, but so far as he knew had not read any.

One-Time Pad: The specimen pad was shown to Oblt. Schubert, who did not recognise it. It was not a Russian army type such as those he had seen, which were bound more securely, to ensure that no pages were lost, and moreover had 20 lines, with 10 groups per line. The only pads he had seen with 5 groups per line were NKGB and some English pads, neither of which had 14 lines per page.

Word-Codes: Asked about word codes, he said these were mainly used by forward units, panzers, etc., and were dealt with in the field, as it would have taken too long to send the material back to OKH and then forward again. These word-codes (Tarntafeln) consisted of words representing set phrases, names of units, numbers, etc.

DECLASSIFIED
Authority NW 48901

I26

TOP SECRET "U"

PAPER WRITTEN BY OBLT. SCHUBERT ON RUSSIAN AGENTS' SYSTEMS

ON THE CYPHER-SYSTEMS OF THE RUSSIAN PARTISANS AND SPIES

In the W/T traffic of the Russian Partisans and spies there were used:

1) Double Transposition
2) Subtractor Recyphers
3) Occasional simple substitution system.

The subtractor systems are covered here in more detail. These consist of 3 Cypher-elements:

1) The basic cypher i.e. the substitution of the plain text by a substitution system
2) The recypher with the figure subtractor
3) The recyphering of the indicators.

The various types of these elements will be dealt with separately.

I. The Basic Cypher

a) On certain links a 3 or 4-figure code was used as basic cypher.

b) In general, however, simple substitution systems were used, which substituted a 1 or 2-figure number for each letter, and were such that seven letters, which usually formed a key-word, were substituted by single figures, and the other three figures were used as tens for the other letters.

Example:

	1	2	3	4	5	6	7	8	9	0	
	S		A		M		O	L	E	T	thus A = 3
2	B		V	G	D	zh	Z	I	K	N	etc. V = 23 etc.

Special points of this substitution system are:

1) When plain text is encyphered by this system, in the cypher text 2 mostly, or all three, tens-figures occur with particular frequency. The frequencies of the figures vary.

2) A letter is not substituted by two like letters. For example, the squares 22, 44, 66 are empty. Thus in normal text no figure can come three times in succession.

3) Numbers are recyphered by repeating each figure three times: e.g. 1945 = 111999444555.

There are two ways of using this system:

1) The basic cypher is the same for all messages.

2) The basic cypher is variable, i.e. it changes from message to message, with the indicator. The indicator is made up of 5 different figures. These are written over the letters of the key and completed with the remaining 5 figures. The tens-figures are taken from the empty squares.

DECLASSIFIED
Authority NW 48901

126

TOP SECRET "U"

Example:

Indicator 37245

3	7	2	4	5	1	6	8	9	0
S		A		M		O	L	E	T
7		B	V	G	D	etc.			
4		P	R	U		F	etc.		

c) There are occasional simple substitution systems which substitute each letter by a 2-figure number.

II. The Composition of the Subtractor

The figure subtractors used are of 3 different kinds:

1) They are printed on T/P rolls
2) They are taken from tables
3) They are built up from an indicator.

1) The subtractors printed on T/P rolls were the most frequently used, and increasingly replaced the other systems. (Russian name: "Bloknot rulon"). The instructions for use lay it down that each recyphering strip is to be destroyed when it has been used once. There are different rolls for "in" and "out" messages. Thus an unbreakable individual recyphering is achieved. A subtractor group from the roll, which is not used for recyphering and is sent in clear, gives the starting point of the strip of the roll used.

Research into regularities in captured subtractor rolls showed:

1) The rolls are made up on several machines (several type-faces).
2) Longish repeats do not occur in a roll.

The rolls have 5-figure numbers, which are given in clear as indicators in Partisan traffic, not in Spy-traffic.

2) The use of subtractor tables comprises in the main 4 systems:

a) There is a simple recyphering with a table of 100-300 groups. The starting point is given by an indicator which gives line and column of the first recypher group: e.g. 11511 = line 11, column 5. Systems of this kind come especially in the traffic of NKGB Leningrad (Solved).

b) There are 100 recypher pages. The first two figures of a 5-figure indicator, made up of 5 different figures, gives the page used. At the same time the basic cypher is changed by the indicator. This system too occurred especially in the traffic of NKGB Leningrad (Solved).

c) There is a double recypher. For this there is a table of 30 lines of 10 groups. The first recypher is taken from the first 18 lines, the second from lines 19-30. The starting point of the first recypher is given by an indicator (as in a)): the second recypher always begins with the first group of the 19th line (Solved).

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

There were besides other isolated systems using independent double recypherment.

d) The system is shown by an example. Two groups are taken from a simple subtractor table, at a starting point given by the indicator: e.g.

27395 80112

To these numbers, according to their numerical value, are allocated the numbers from 1 to 0:

37596 80124
27395 80112

From this is obtained, by mixing and dividing off:

3	7	5	9	6	8	0	1	2	4
3	27	753	9	96	588	0	01	121	42

The following groups in the subtractor table are next changed. This gives the recypher (Not solved).

[Note: The marking off into blocks of 1, 2 and 3 figures was apparently done to transpose the figures in these blocks according to the key provided by the top line]

3) Figure-subtractors arithmetically constructed. The subtractors are built up from a five figure indicator, which contains 5 different figures. The methods of building them up will be demonstrated by examples.

a) Simple addition in columns. The most usual type of this subtractor construction are the following: There are two substitution series, e.g.:

	1	2	3	4	5	6	7	8	9	0
a	0	9	1	8	3	6	2	5	4	7
b	7	6	8	2	0	1	9	4	3	5

The indicator, e.g. 27345 is written down, then substituted according to a), and the result written underneath. Then the indicator is substituted according to b) and the answer written at the side on the right:

27345 69820
92183

The groups on the left are now added, and the result written under on the right. Then the two groups on the right are added, and the result put below on the left, and so on:

27345 69820
92183 19428
78248 60321
79749 47987
07208 ----- etc.

The groups are used as Subtractor, starting from the second or third line. In some systems the right hand column is pushed down a line (Solved). In some cases the substitution series b) is derived from a) by pushing it along one or more places. The case also occurred of there being only one substitution series, with addition in one column only.

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

126

b) Simple cross addition. Starting with the indicator, each pair of adjacent figures is added, and the result written alongside.

Example:

Indicator	27345			
Subtractor	27345	90794	97633	63969

This system occurred only as an emergency cypher (Solved).

There is a variation, in which one skips a figure:

27345 51896 30426

or one may add in normal fashion three times and then skip a figure twice:

27345 90735 97022 .....

These last systems were used in conjunction with a changing basic cypher (Solvable).

c) Addition in columns with a key phrase. The basic key varies with the indicator. A key group or phrase is encyphered in accordance with the basic key so that 5 groups of 5 are produced. The indicator is written under the first of these groups, the total of these two groups is put under the adjacent one, and so on.

49458	03243	56083	03824	26493
27345	66793	69936	15919	18733

The subtractor is obtained either by adding these two rows and every subsequent row being the total of the last two rows or by continuing the addition (Solved).

d) Cross addition with key phrase. By encyphering a key phrase with the fixed basic key, you have 5 - 5-figure groups. The indicator is written under the first of these groups; as the next group you take the missing 5 numbers in ascending order and by cross addition, the five groups are filled in.

The first row of the subtractor is produced by adding both rows.

Example:

Key Phrase	49458	03243	56083	03824	26493
Indicator	27345	16890	90796	74799	97653
1 Subtractor Row	66793	19033	46779	77513	13046

By cross addition of the groups of the first subtractor row, 4 groups are formed for each original group and these are entered underneath. You then get a block of 25 groups

66793	19033	46779	77513	13046
23625	09363	03469	42647	43400
59870	92992	37052	68013	77407
47574	11813	07572	48147	41471
12215	29945	72299	29519	55188

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

126

From the first group of the block a key is made up by indicating the figures according to numerical orders by the numbers 1 - 5.

23451
66793

In accordance with this key the columns are read out from the columns of the first subtractor block, commencing with the right column. From this one gets the second subtractor block:

60718	14745	33715	04441	40078
37379	74642	72889	56015	14141
99229	40307	63772	74052	76579
33235	etc.			

The third subtractor block comes correspondingly from the second by re-arranging the second group of the first subtractor row (Solved).

In a variation of this system, the first subtractor block is composed differently, the first subtractor row is exactly the same. The cross addition from the indicator is, however, extended to 6 groups. The sixth group is put under the first subtractor group. After that the formation of the subtractor proceeds as described under c) (Solved). In this last type variable basic keys are also used (Soluble).

e) Substituted cross addition. The indicator is substituted by a table. Five groups are formed by cross addition from the result. These are then converted by the same, or a different, substitution table. From this you obtain the first subtractor row. From this point on, the procedure is as under d) (Solved).

f) Subtractor Boxes. First the figures 1 - 0 are written down and underneath, the indicator and remaining figures. By adding every two rows, 9 further rows are formed. The 2 - 11th row are numbered 1 - 0.

Example:

	1	2	3	4	5	6	7	8	9	0
1)	2	7	3	4	5	1	6	8	9	0
2)	3	9	6	8	0	7	3	6	8	0
3)	5	6	9	2	5	8	9	4	7	0
4)	8	5	5	0	5	5	2	0	5	0
5)	3	1	4	2	0	3	1	4	2	0
6)	1	6	9	2	5	8	3	4	7	0
7)	4	7	3	4	5	1	4	8	9	0
8)	5	3	2	6	0	9	7	2	6	0
9)	9	0	5	0	5	0	1	0	5	0
0)	6	3	7	6	5	9	8	2	1	0

When figure pairs are extracted from a particular row, e.g. row 3, and these indicate from which point each 5 figure group is to be read out of the box. This produces:

56 = 31420
69 = 70169
92 = 05050 etc.

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

126

This system appeared in conjunction with the variable basic key. A variation consists in a key phrase being encyphered on a basic key and from this the two first rows of the box are formed (Not solved). Recognition of the subtractor system and its solution was achieved by the appearance of similar message endings and beginnings (Similar addresses and signatures).

III. Indicators

Indicators for the subtractor, based on a roll, were always inserted "plain". In the other systems there were several ways of putting in the indicator. Apart from a very few exceptions there were always two indicators. Possibilities regarding recyphering of these indicators were as follows:

1) Indicator groups plain

2) A certain 5-figure number is added to every indicator and the number is constant.

3) A certain group of the message is added to every indicator group.

4) Like 3) with the difference that groups in the message are converted according to a substitution table.

5) Like 4), where different substitution tables are used for the two groups of the message to be converted.

6) Like 3), except that figures of the message groups are arranged in order and then added to the indicator group.

7) Certain figures are extracted from several groups of the message (almost invariably the first 5 groups), for instance, the last figures of the first 5 groups and then added to the indicator group.

8) Like 7), but substituting the adders in accordance with a substitution table.

9) Combinations of two of the above methods (doubled recypher of indicator groups): 2 with 3, 2 with 4, 2 with 5, twice 3.

In general both indicators are recyphered on the same process, where one indicator is included at the beginning and one at the end of a message. The groups used for encyphering are also taken one each from beginning and end of the message.

Re cypher was broken:

1) When both indicators were encyphered on the same system.

2) When there were messages on the same key.

3) Methods 2), 3), 4), 5), when indicators consisted of 5 different figures.

4) When the indicator was known by virtue of other circumstances (Solution of the subtractor without knowing the indicators).

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

I26

When substitution tables were used to make up the subtractor and to encypher the indicators, it happened occasionally that the same tables were used.

Messages often contained other groups together with the indicators such as date, message no., number of groups in the message or recognition number of the sender. These groups were plain or were recyphered by adding a group in the message.

The above gives the most important cyphers used by Russian Partisans and spies, as far as they are known from breaks, captured documents and POW statements. Systems used in the Balkans are not included but they are of a similar type. After the middle of '44, W/T traffic of the partisans and spies dropped heavily, as they were constantly being overtaken by the advance of the Red Army.

CONCERNING CYPHERS AND CODES OF THE POLISH NATIONAL RESISTANCE MOVEMENT

In the following account, codes and cyphers of the Polish National Resistance Movement (ARMIJA KRAJOWA) are covered. These were directed by the Polish Government in London. The following processes were first worked on at OKH during the Warsaw Rising. Previously only the 5-figure key in London-Warsaw traffic was read at OKW/Chi.

These were:

1) Letter traffic encyphered by a simple transposition (Solved) and by double transposition (Unsolved).

2) 4-letter traffic, not worked on at OKH.

3) 3-letter traffic, about which more is given below.

There was amongst this a simple 2-figure substitution cypher without an indicator. Cyphers 066, 090, 117, 118, 181 were broken. Others were being worked on.

I shall attempt to describe the cyphers broken as far as my memory serves. The simplest cypher 066 in its old form. The clear text was written into a square 10 x 12. Letters were taken out of these squares in columns and in order, and converted into figures by a 2-figure substitution process. The text was passed in 3-figure groups.

The substitution looked approximately like this:

A	B	E	H	M	T	A	G	P	Ø
Ą	D	G	Ł	S	Z	F	O	9	Z
C	F	L	R	Y	Ę	N	8	Y	8
Ę	K	P	X	E	M	7	X	7	-
I	O	W	D	Ł	6	W	6	-	-
N	V	C	L	5	V	5	NR	-	-
U	B	K	4	V	4	(,)	-	-	-
Ą	I	3	T	3	(.)	-	-	-	I
H	2	S	2	Ø	-	-	-	E	U
1	R	1	9	-	-	-	A	O	Y

(approx.)

Daily changing figure strips were laid on this. The horizontal strip was drawn from the first 10 letters of the date, and the vertical was obtained by adding a certain figure to the horizontal. The horizontal strip was arranged differently for each square so that occasionally 1, 2, 3, 4, stood in order over the first column. In the first cage the figures stood over the first column which had to be added to obtain the vertical strip from the horizontal one. The indicators showed:- Date (day and month), length of the message in letters and the figures to be added. Together with the length of the message, they also gave the number of letters in the last cage. The indicators stood at the beginning and end of the message and were encyphered by adding groups in the message. This system was altered by moving the vertical strip from column to column in the cage.

DECLASSIFIED
Authority NW 48901

TOP SECRET "U"

126

The remaining systems are evolved on similar lines. There are the following variations:

1) Different basic key.

2) The figure strips are not drawn from the date but from key phrases. Both strips are drawn up independently of one another. In cypher 090 the process is done from a 3-figure group, given as an indicator.

3) Both strips are moved from column to column in the cage.

4) The strips are not applied in ascending numerical order, but either the sequence of the figures to be applied is taken from the other strip or it is fixed specially. Sequences of the figures to be applied have a period of 10 for one list and for the other a period of 9 or longer.

5) Key lengths (widths of cage) of No. 436 (?), in which I imagine letter pairs are read from the cages and are encyphered according to a variable 3-figure substitution process.

RP

SECRET 19.6.45.

Paper written by Oblt Schubert on Russian Agents' Systems.

68452
CBQK 2

UEBER SCHLUESSELVERFAHREN DER RUSSISCHEN PARTISANEN UND KUNDSCHAFTER.

Im Funkverkehr der russischen Partisanen und Kundschafter wurden angewandt:

1) Doppelwuerfel
2) Wurmverfahren
3) Vereingelt einfache Ersatzverfahren

Die Wurmverfahren sollen hier naeher behandelt werden. Diese bestehen aus 3 Schluesselvorgaengen:

1) Dem Grundschluessel, das ist der Ersatz des Klartextes durch ein Ersatzverfahren
2) Der Ueberschluesselung mit dem Zahlenwurm
3) Der Verschluesselung der Kenngruppen

Die verschiedenen Arten dieser Schluesselvorgaenge werden getrennt aufgefuehrt.

I. Die Grundschluessel.

a) In bestimmten Verkehren wurde ein 3- oder 4-stelliger Zahlencode als Grundschluessel benutzt.
b) Im allgemeinen wurden jedoch einfache Ersatzverfahren angewandt, die jeden Buchstaben durch eine 1- oder 2-stellige Zahl ersetzten, und zwar derart, dass sieben Buchstaben, die meist ein Kennwort bildeten, durch einstellige Zahlen ersetzt wurden, die uebrigen 3 Ziffern wurden als Zehner fuer die uebrigen Buchstaben benutzt. Beispiel:

	1	2	3	4	5	6	7	8	9	0	
	S		A		M	Ä	O	L	E	T	also A = 3
2	B		V	G	D	zh	Z	J	K	N	usw. V = 23

usw.

Besonderheiten dieses Ersatzverfahrens sind:

1) Wird ein Klartext danach verschluesselt, so fallen im verschluesselten Text meist 2 oder alle 3 Zehnerziffern durch besondere Häufigkeit auf. Die Haeufigkeiten der Ziffern sind verschieden.

2) Ein Buchstabe wird nicht durch zwei gleiche Ziffern ersetzt. Zum Beispiel sind die Felder 22, 44, 66 nicht belegt. Dadurch kann im normalen Text keine Ziffer 3-fach hintereinander auftreten.

3) Zahlen werden so verschluesselt, dass jede Ziffer dreifach gesetzt wird, z.B. 1945 = 111999444555.

Zu der Anwendung dieses Verfahrens traten zwei Moeglichkeiten auf:

1) Der Grundschluessel ist fuer alle Sprueche der gleiche.
2) Der Grundschluessel ist veraenderlich, d.h. er wechselt von Spruch zu Spruch, mit der Kenngruppe.

Die Kenngruppe besteht aus 5 verschiedenen Ziffern. Diese werden ueber die Buchstabenanordnung des Schluessels geschrieben und durch die restlichen 5 Ziffern aufgefüllt. Die Ziffern fuer die Zehner entnimmt man aus den leeren Feldern. Beispiel:

Kenngruppe 37245

	3	7	2	4	5	1	6	8	9	0
	S		A		M		O	L	E	T
7	B	V	G	D	usw					
4	P	R	U	.	F	"				

c) Vereinzelt treten einfache Ersatzverfahren auf, bei denen jeden

Un 201401 by NW
DECLASSIFIED
Authority NW 48901

DECLASSIFIED
Authority NW 48901

Buchstabe durch eine 2-stellige Zahl ersetzt wird.

II. Die Bildung des Zahlenwurms.

Die benutzten Zahlenwuermer entstehen auf 3 verschiedene Arten:

1) Sie sind auf Fernschreiberrollen vorgedruckt
2) Sie werden Tafeln entnommen
3) Sie werden durch Rechnung aus einer Kenngruppe entwickelt.

1) Die auf Fernschreiberrollen vorgedruckten Wuermer wurden am haeufigsten angewandt und loesten die anderen Systeme mehr und mehr ab. (Russische Bezeichnung: "Bloknot rulon"). Die Anwendungsvorschrift besagt, dass jeder zur Verschluesselung benutzte Streifen der Rolle nach einmaligem Gebrauch zu vernichten ist. Fuer ein- und ausgehende Sprueche bestehen verschiedene Rollen. Es wird damit eine unloesbare individuelle Verwuermung erreicht. Eine im Spruch offen stehende Wurmgruppe der Rolle, die zur Ueberschluesselung nicht benutzt wird, gibt den Anfang des benutzten Rollenstreifens an.

Untersuchungen ueber Gesetzmaessigkeiten des Wurmes ergaben:

1) Die Rollen sind auf verschiedenen Maschinen hergestellt (verschiedene Drucktypen).
2) Laengere Wiederholungen kommen auf eine Rolle nicht vor.

Die Rollen tragen 5-stellige Nummern, die im Partisanenspruechen, nicht in Kundschafterspruechen, offen angegeben sind.

2) Bei der Verwendung von Wurmtafeln treten im Wesentlichen 4 Systeme auf:

a) Es liegt eine einfache Verwurmung mit einer Tafel von 100 bis 300 Wurmgruppen vor. Der Beginn des Wurmes wird durch eine Kenngruppe angegeben, die Zeile und Spalte der ersten Wurmgruppe angibt, z.B. 11 5 11 = 11. Zeile, 5. Spalte. Derartige Verfahren treten besonders in Verkehr des NKGB Leningrad auf. (Geloest).

b) Es bestehen 100 Wurmseiten. Durch die ersten beiden Ziffern einer 5-stelligen Kenngruppe, die 5 verschiedene Ziffern enthaelt, wird angegeben, welche Seite benutzt wird. Gleichzeitig wird der Grundschluessel durch die Kenngruppe veraendert. Dieses Verfahren trat ebenfalls besonders im Verkehr des NKGB Leningrad auf. (Geloest).

c) Es liegt eine Doppelverwurmung vor. Dazu besteht eine Tafel von 30 Zeilen zu 10 Gruppen. Aus den ersten 18 Zeilen wird der erste Wurm, aus dem 19. - 30. Zeilen entnommen. Der Beginn des ersten Wurms wird durch Kenngruppe angegeben, wie unter a), der zweite Wurm beginnt immer mit der ersten Gruppe der 19. Zeile. (Geloest).

Daneben bestanden vereinzelt noch andere Systeme unabhaengiger doppelter Verwurmungen. MKK

d) Das Verfahren wird an einem Beispiel erklaert. Aus einer einfachen Wurmtafel werden von einem durch die Kenngruppe angegebenen Einsatzpunkt zwei Gruppen entnommen. z.B.

27395 80112

Diesen Ziffern werden der Groesse nach die Ziffern von 1 bis 0 zugeordnet:

DECLASSIFIED
Authority NW 42901

37596 80124
27395 80112

Daraus entsteht, durch Mischen und Abteilen:

3 7 5 9 6 8 0 1 2 4
3/ 2 7/ 7 5 3/ 9/ 9 6/ 5 8 8/ 0/ 0 1/ 1 2 1/ 4 2

Die folgenden Gruppen der Wurmtafel werden danach getauscht. Damit erhaelt man den Wurm. (Nicht geloest).

3) Durch Rechnung entwickelte Zahlenwuermer. Die Wuermer werden aus einer 5-stelligen Kenngruppe entwickelt, die 5 verschiedene Ziffern enthaelt. Die Methoden der Aufstellung werden an Beispielen durchgefuehrt.

a) Einfache Addition in Kolonnen. Die gebraeuchlichsten Arten dieser Wuermerstellungen sind folgende: es liegen zwei Tauschreihen vor, z.B.

	1	2	3	4	5	6	7	8	9	0
a	0	9	1	8	3	6	2	5	4	7
b	7	6	8	2	0	1	9	4	3	5

Die Kenngruppe, z.B., 27345, wird hingeschrieben, danach nach a) getauscht, und das Ergebnis darunter geschrieben. Dann wird die Kenngruppe nach b) getauscht, und diese Tauschwert rechts daneben geschrieben:

2 7 3 4 5 6 9 8 2 0
9 2 1 8 3

Nun werden die linken Gruppen addiert, und das Ergebnis rechts untergesetzt. Dann werden die beiden rechten Gruppen addiert, und das Ergebnis links untergesetzt, usw:

2 7 3 4 5 6 9 8 2 0
9 2 1 8 3 1 9 4 2 8
7 8 2 4 8 6 0 3 2 1
7 9 7 4 9 4 7 9 8 7
0 7 2 0 8 . . . . usw.

Die Gruppen werden, von der zweiten oder dritten Zeile beginnend, als Wurm benutzt. Bei einigen Verfahren ist die rechte Kolonne um eine Zeile nach unten verschoben. (Geloest). In einigen Faellen entsteht die Tauschreihe b aus a durch Verschiebung um eine Stelle. Es kam trat auch der Fall auf, dass nur eine Tauschreihe vorlag, und die Addition in nur einer Kolonne erfolgte.

b) Einfache Queraddition. Darum entsteht aus der Kenngruppe dadurch, dass je 2 benachbarte Ziffern addiert werden, und das Ergebnis hinten angefuegt wird. Beispiel:

Kenngruppe 2 7 3 4 5
Wurm 2 7 3 4 5 9 0 7 9 4 9 7 6 3 3 6 3 9 6 9

Dieses Verfahren trat nur als Notschluessel auf (Geloest). Eine Abwandlung besteht darin, dass man eine Ziffer dabei ueberspringt:

2 7 3 4 5 5 1 8 9 6 5 0 4 2 6

oder dass man dreimal normal addiert, und dann zweimal eine Ziffer ueberspringt:

2 7 3 4 5 9 0 7 3 5 9 7 0 2 2 ...

Diese letzten Verfahren traten in Verbindung mit wechselndem Grundschluessel auf (loesbar).

DECLASSIFIED
Authority NW 48901

c) Kolonnenadditionen mit Schluesselsatz. Der Grundschluessel wechselt mit der Kenngruppe. Nach dem Grundschluessel wird ein Schluesselsatz verschluesselt, sodass fuenf 5-Gruppen entstehen. Unter die erste dieser Gruppen wird die Kenngruppe gesetzt, die Summe dieser beiden Gruppen unter die naechste und so weiter:

49458 03243 56083 03824 26493
27345 06793 69936 15919 13733

Der Wurm entsteht entweder dadurch, dass diese beiden Zeilen addiert werden und jede folgende Zeile als Summe der beiden letzten Zeilen entsteht oder dass das Additionsverfahren weiter fortgesetzt wird (loesbar).

d) Queraddition mit Schluesselsatz. Durch Verschluesselung eines Schluesselsatzes mit dem festen Grundschluessel entstehen fuenf 5-Gruppen. Unter die erste dieser Gruppen schreibt man die Kenngruppe, nimmt als naechste Gruppe die fehlenden fuenf Ziffern in steigender Folge und fuellt durch Queraddition auf fuenf Gruppen auf. Durch Addition beider Zeilen entsteht die erste Wurmzeile, Beispiel:

Schluesselsatz	49458	03243	56083	03824	26493
Kenngruppe	27345	16890	90796	74799	97655
1. Wurmzeile	66793	19033	46779	77513	13046

Aus den Gruppen der ersten Wurmzeile werden durch Queraddition je vier Gruppen gebildet, die untergesetzt werden. Damit entsteht ein Block von 25 Gruppen:

66793 19033 46779 77513 13046
23625 09363 05469 42647 43400
59870 92992 37052 68013 77407
47574 11813 07572 48147 41471
12215 29945 72299 29519 55188

Nun erstellt man aus der ersten Gruppe des Blocks eine Losung indem man die Zahlen der Groesse nach mit den Ziffern von 1 - 5 bezeichnet:

23451
66793

Nach dieser Losung liest man innerhalb der Kolonnen des ersten Wurmblocks die Spalten heraus, wobei man mit der rechten Kolonne beginnt. Man erhaelt dadurch den zweiten Wurmblock:

60718 14745 33715 04441 40078
37379 74642 72889 56015 14141
99229 40307 63772 74052 76579
53235 u. s. w.

Der dritte Wurmblock entsteht aus den zweiten entsprechend durch Umordnung der zweiten Gruppe der ersten Wurmzeile. (Geloest).
In einer Abart dieses Verfahrens wird der erste Wurmblock anders gebildet. Die erste Wurmzeile entsteht genauso. Die Queraddition aus der Kenngruppe wird jedoch bis auf 6 Gruppen ausgedehnt. Diese sechste Gruppe wird unter die erste Wurmgruppe gesetzt. Nun verlaeuft die weitere Wurmbildung wie unter c). (Geloest). In dieser letzten Art werden auch wechselnde Grundschluessel benutzt (loesbar).

e) Getauschte Queraddition. Die Kenngruppe wird nach einer Tauschreihe getauscht. Aus dem Ergebnis werden durch Queraddition fuenf Gruppen gebildet. Diese werden nach der gleichen oder einer anderen Tauschreihe getauscht. Dadurch entsteht die erste Wurmzeile. Die weitere Bildung verlaeuft wie unter d). (geloest).

f) Wurmkasten. Zuerst werden die Ziffern von 1 bis 0 hingeschrieben darunter die Kenngruppe und die restlichen Ziffern. Durch Addition je zweier Zeilen werden weitere 9 Zeilen gebildet. Die 2. bis 11. Zeile erhalten die Ziffern 1 bis x 0. Beispiel:

	1	2	3	4	5	6	7	8	9	0
1)	2	7	3	4	5	1	6	8	9	0
2)	3	9	6	8	0	7	3	6	8	0
3)	5	6	9	2	5	8	9	4	7	0
4)	8	5	5	0	5	5	2	0	5	0
5)	3	1	4	2	0	3	1	4	2	0
6)	1	6	9	2	5	8	3	4	7	0
7)	4	7	3	4	5	1	4	8	9	0
8)	5	3	2	6	0	9	7	2	6	0
9)	9	0	5	0	5	0	1	0	5	0
0)	3	3	7	6	5	9	8	2	1	0

Nun werden einer bestimmten Zeile, z.B. der Zeile 3), Ziffernpaare entnommen, die angeben von wo aus je 5-stellige Gruppen aus dem Kasten herausgelesen werden sollen, dies gibt:

56	M =	3	1	4	2	0
69	=	7	0	1	6	9
92	=	0	5	0	5	0 usw.

Dieses Verfahren trat in Verbindung mit wechselnden Grundschluessel auf (Loesbar). Eine Abart dieses Verfahrens besteht darin, dass nach dem Grundschluessel ein Schluesselsatz verschluesselt wird, und damit die beiden ersten Zeilen des Kasten gebildet werden. (Loesung nicht gelungen). Das Erkennen der Wurmverfahren und die Loesung gelang durch das Auftreten gleicher Spruchanfänge und -schluesse (Gleiche An- und Unterschriften).

III. Kenngruppen.

Die Kenngruppen fuer den Wurm, der einer Rolle entstammte, wurden immer offen gesetzt. Fuer die uebrigen Verfahren existierten mehrere Arten, die Kenngruppen zu setzen. Von ganz wenigen Ausnahmen abgesehen wurden immer zwei Kenngruppen gesetzt. Die Moeglichkeiten der Ueberschluesselung dieser Kenngruppen waren folgende:

1) Die Kenngruppen stehen offen.

2) Zu jeder Kenngruppe wird eine bestimmte 5-stellige Zahl addiert, die sich nicht aendert.

3) Zu jeder Kenngruppe wird eine bestimmte Gruppe des Spruches addiert.

4) Wie 3), mit dem Unterschied, dass die Spruchgruppen nach einer Tauschreihe getauscht werden.

5) Wie 4), wobei fuer die beiden zu tauschenden Spruchgruppen verschiedene Tauschreihen benutzt werden.

6) Wie 3), mit dem Unterschied, dass die Ziffern der Spruchgruppen der Groesse nach geordnet und dann addiert werden.

7) Es werden aus mehreren Spruchgruppen (fast immer die ersten 5 Gruppen) bestimmte Ziffern herausgegriffen, beispielsweise die letzten Ziffern der ersten 5 Spruchgruppen, und dann addiert.

8) Wie 7), jedoch mit Tausch der zu addierenden Ziffern nach einer Tauschreihe.

9) Kombinationen zweier der vorangehenden Verfahren (doppelte Ueberschluesselung der Kenngruppen): 2 mit 3, 2 mit 4, 2 mit 5, zweimal 3.

DECLASSIFIED
Authority NW 48901

Im Allgemeinen wurden beide Kenngruppen nach demselben Verfahren ueberschluesselt, wobei eine Kenngruppe im Anfang, eine im Schluss des Spruches enthalten war. Die zur Verschluesselung benutzten Spruchgruppen werden ebenso je eine aus dem Anfang und je eine aus dem Schluss des Spruches entnommen.

Die Ueberschluesselung wurde geloest,

1) Wenn beide Kenngruppen nach dem gleichen Verfahren verschluesselt waren.

2) Wenn Schluesselgleiche Sprueche vorlagen.

3) Die Methoden 2), 3), 4), 5), wenn die Kenngruppen aus 5 verschiedenen Ziffern bestanden.

4) Wenn die Kenngruppe durch andere Umstaende bekannt war. (Loesung des Wurmes ohne Kenntnis der Kenngruppen.

Wenn zur Bildung des Wurmes und zum Verschluesseln der Kenngruppen Tauschreihen benutzt wurden, wurden jeweils dieselben Reihen dazu verwandt.

Neben diesen Kenngruppen enthielten die Sprueche oft noch andere Gruppen, die Datum, Spruchnummer, Gruppenzahl des Spruches oder Erkennungsnummer des Absenders enthielten. Diese Gruppen standen offen oder waren durch Addition einer Spruchgruppe ueberschluesselt.

Damit sind die wesentlichsten Schluesselverfahren der russischen Partisanen und Kundschafter geschildert, soweit sie durch Loesungen, Beutepapiere und Vernehmungen mir bekannt sind. Nicht enthalten sind die auf dem Balkan angewandten Verfahren, die jedoch aehnlicher Art sind. Seit Mitte '44 ging der Funkverkehr der Partisanen und Kundschafter stark zurueck, da diese durch den Vormarsch der Roten Armee wiederholt ueberlaufen wurden.

- - - - - -

UEBER SCHLUESSELVERFAHREN DER NATIONALPOLNISCHEN WIDERSTANDSBEWEGUNG

Es handelt sich im Nachstehenden um Schluesselverfahren der Nationalpolnischen Widerstandsbewegung (Armija Krajowa), die von der polnischen Regierung in London geleitet wurde. Die nachstehenden Verfahren wurden erst im Verlaufe des Warschauer Aufstandes beim OKH bearbeitet. Vorher wurde nur der 5-Zahlen-Schluessel im Verkehr London-Warschau bei OKW/Chi gelesen.

Es traten auf:

1) Buchstaben-Sprueche, die nach einfachem Wuerfel (geloest) und Doppelwuerfel (nicht geloest) verschluesselt waren.

2) 4-Zahlen-Sprueche, die beim OKH nicht bearbeitet wurden

3) 3-Zahlen-Sprueche, auf die hier naeher eingegangen werden soll.

Es befand sich darunter ein einfaches 3-Zahlen Ersatzverfahren ohne Kennnummer. Geloest wurden die Verfahren: 066, 090, 117, 118, 181. Andere waren in Bearbeitung.

Ich will versuchen, die geloesten Verfahren, soweit es aus dem Gedaechtnis moeglich ist, zu beschreiben. Das einfachste Verfahren 066 in seiner alten Form. Der Klartext wird in Wuerfel von 10 x 12 Feldern geschrieben. Aus diesen Wuerfeln werden die Buchstaben spaltenweise der Reihe nach herausgelesen und dabei nach einem 3-Zahlen-Ersatzverfahren in Zahlen umgesetzt. Der Text wird in 5-Zahlen-Gruppen gefunkt.

Das Ersatzverfahren sah etwa folgendermassen aus:

DECLASSIFIED
Authority NW 48901

A	B	E	H	M	T	A	G	P	Ø
Ä	D	G	Z	S	Z	F	O	9	Z
C	F	L	R	Y	E	N	S	X	8
E	K	P	X	E	M	7	X	7	.
I	O	W	D	Z	G	W	6	.	.
N	V	C	L	S	V	5	Nr.	.	.
U	B	K	M	U	4	(,)	.	.	.
Ä	I	3	T	3	( )	.	.	.	I
H	2	S	2	Ø	.	.	.	E	U
1	R	1	9	.	.	.	A	O	Y

(ungefaehr)

Daran wurden Zahlenleisten angelegt, die taeglich wechselten. Die waagerechte Leiste wurde aus den ersten 10 Buchstaben des Datums abgeleitet, der senkrechte entstand durch Addition einer bestimmten Ziffer zur waagerechten. Die waagerechte Leiste wurde von Wuerfel zu Wuerfel anders angelegt, so dass jeweils der Reihe nach 1, 2, 3, 4 ueber der ersten Spalte stand. Fuer den ersten Wuerfel stand die Ziffer ueber der ersten Spalte, die addiert werden musste, um die senkrechte Leiste aus der waagerechten zu gewinnen. Die Kenngruppen gaben an: Datum (Tag und Monat), Laenge des Spruches in Buchstaben, und die zu addierende Ziffer. Nebst der Laenge des Spruches wurde auch die Buchstabenzahl im letzten Wurfel angegeben. Die Kenngruppen stehen im Anfang und im Schluss des Spruches und sind durch Addition von Spruchgruppen verschluesselt. Dieses Verfahren wurde dadurch geaendert, dass die senkrechte Leiste von Wuerfelspalte zu Wuerfelspalte verschoben wurde.

Die uebrigen Verfahren sind entsprechend aufgebaut. Es treten folgende Abwandlungen auf:

1) Anderer Grundschluessel.
2) Die Zahlenleisten werden nicht aus dem Datum abgeleitet, sondern aus Schluesselsaetzen. Die beiden Leisten sind voneinander unabhaengig abgeleitet. Beim Verfahren 090 erfolgt die Ableitung aus einer 3-stelligen Zahl, die als Kenngruppe angegeben wird.
3) Es werden von Wuerfelspalte zu Wuerfelspalte beide Leisten verschoben.
4) Die Leisten werden nicht der Reihe nach mit steigenden Zahlen angelegt, sondern entweder wird die Folge der anzulegenden Zahlen der anderen Leiste entnommen, oder sie ist besonders festgelegt. Die Folgen der anzulegenden Zahlen hat fuer eine Leiste die Periode 10, fuer die andere die Periode 9 oder laenger.
5) Die Wuerfelbreiten des Nr. 436 (?), bei dem vermutlich Buchstabenpaare aus den Wuerfeln herausgelesen wurden, die nach einem wechselnden 3-Zahlenersatzverfahren verschluesselt wurden.

DECLASSIFIED
Authority NW 48901

Supplementary notes on Oblt. SCHUBERT, OKH. (17.6.45 to 20.6.45)

(a) Protokoll vom 17.6.45.

p.1 Note (1) He was Kommandeur der Nachrichtenaufklaerung 6. Each regiment was designated by a number, and its particular Nachrichtenaufklaerungskompanie took that number.

(2) There were actually three branches of the Ostentzifferung OKH: (1) Heer, (2) NKWD (3) Partisan

(3) should read: Da waren Felder von 10 x 10, die Buchstaben und Zahlen enthielten. Die Ueberschluesselungsleisten wechselten taeglich.

(These Leisten were strips containing co-ordinates for the sides of the square, e.g.

2 6 9 4 3 1 8 7 5 0 2 6 9 4 3 1 8 7 5 0

These could be slid according to an order indicated by the Kenngruppe.

p.2 (4) These two paragraphs are two descriptions of the same thing. The code book was cut away at the top and side margins, position ~~xxxxxxxxx~~ co-ordinates for the pages being printed on the cover. At the bottom, the pages were thumb-indexed, page 00 having, for example, 11-23, and so on:

/11-23 /00-10 /36-46/ 82-94/

The Systemquadrat mentioned at the foot of page 2 was a latin square of numbers, 10 x 10.

p.3 (5) This indicator system is described more fully on p4. The first bigram usually indicated the recipher table for the page, the third figure the number to be added to the second margin co-ordinate, and the fourth figure the recipher table for the margin after the addition indicated by the third figure.

(6) should read: ganz vereinzelt 4 bis 7 Ersatzsysteme (i.e. 4 to 7-figure substitution systems)

p.6 (7) This subject is dealt with more fully in Oblt. Schubert's paper on Agents' Systems.

(8) ditto.

- - - - - - - - - - - - - - - - -

DECLASSIFIED
Authority NW 48901

Supplementary notes -

Oblt. Schubert was asked to describe the different links on which the various Agents' systems were used. He said he could not remember enough to give details, which were in many cases not known. In the middle of last year, for example, the Russians had, he thought, about 3,000 agents spread over all areas, and it was impossible to pick out one system and say that was used in one area. Moreover, he himself had only worked on Partisan traffic and Kundschafter, and knew of other systems (e.g. Balkan) only indirectly.

Machines: Oblt. Schubert said he himself had never worked on machines, which were dealt with by the machine section. The Russians had a machine in use already at the beginning of the war, but not on military traffic. Recently there had been small quantities of 5-letter military traffic, but not enough to work on, and they had no idea of the system.

The T/P traffic had been worked on in the machine section, and he thought messages in depth had been read; he did not know whether the machine had been recovered.

- - - - - - - - - - -

Regarding Agents' Traffic, he mentioned that in January this year a Reg. Rat (? Ober Reg. Rat) WENZEL was sent to him from the Forschungsamt by WNV Fu 3, which was in charge of Agents' systems, with the object of collaborating with him on Polish Resistance Movement traffic. Schubert knew the Forschungsamt had worked on Polish systems, but so far as he knew had not read any.

One-time pad: The specimen pad was shown to Oblt. Schubert, who did not recognise it. It was not a Russian army type such as those he had seen, which were bound more securely, to ensure that no pages were lost, and moreover had 20 lines, with 10 groups per line. The only pads he had seen with 5 groups per line were NKGB and some English pads, neither of which had 14 lines per page.

Word-Codes: Asked about word codes, he said these were mainly used by forward units, panzers etc., and were dealt with in the field, as it would have taken too long to send the material back to OKH and then forward again. These word-codes (Tarntafel) consisted of words representing set phrases, names of units, numbers etc.